PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-297541
(43)Date of publication of application : 11.10.2002

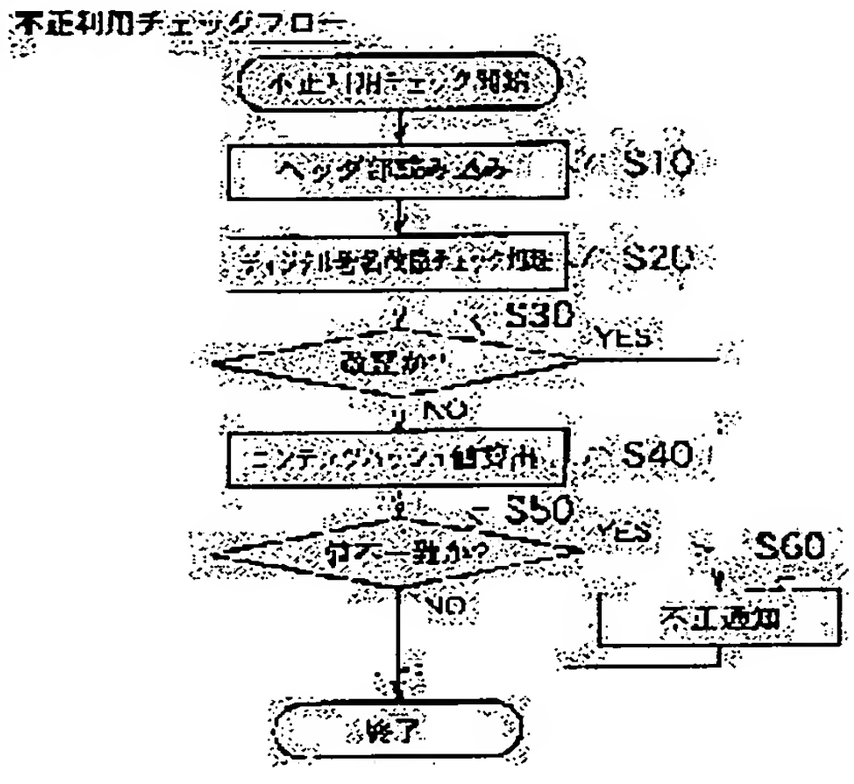
(51)Int.CI. G06F 15/00
G09C 1/00

(21)Application number : 2001-102393
(22)Date of filing : 30.03.2001

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KUROKAWA KIYOSHI
AZUMA SHOZO
SANO MUTSUO

(54) UNAUTHORIZED UTILIZATION NOTICE METHOD, ITS DEVICE AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an unauthorized utilization notice method, its device and program capable of monitoring unauthorized utilization for contents downloaded freely at a client-side without making a user be conscious.
SOLUTION: This method comprises: reading a hash value of contents described before the circulation from a contents ID attached to the contents after circulation (S10); calculating a hash value of contents for the contents after the circulation by using the same hash function as the hash function used in calculation of the hash value of contents described before the circulation (S40); determining whether the unauthorized utilization is present depending on whether the hash value of contents before-and-after the circulation are matched with each other (S50); and sending the unauthorized utilization information indicating the unauthorized utilization in an address of a management server included in contents ID when the unauthorized utilization is present (step S60).



LEGAL STATUS
[Date of request for examination]
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開２００２－２９７５４１
(P２００２－２９７５４１A)
(43)公開日　平成14年10月11日(2002.10.11)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０　Ａ	5B085
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０　Ａ	5J104
					６４０　Ｄ	

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願2001-102393(P2001-102393)

(22)出願日　平成13年3月30日(2001.3.30)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目3番1号

(72)発明者　黒川　清
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内

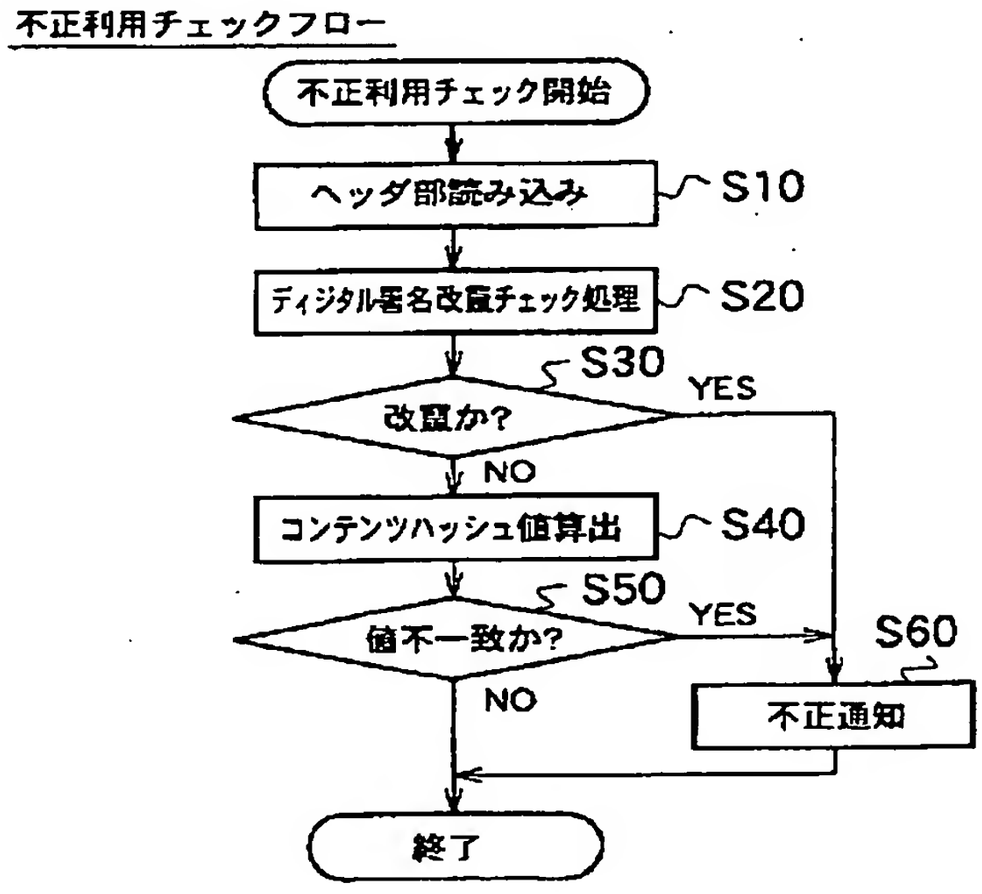
(72)発明者　東　正造
東京都千代田区大手町二丁目3番1号　日本電信電話株式会社内

(74)代理人　100083806
弁理士　三好　秀和　（外1名）

最終頁に続く

(54)【発明の名称】不正利用通知方法、不正利用通知装置および不正利用通知プログラム

(57)【要約】
【課題】　本発明は、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知プログラムを提供することにある。
【解決手段】　流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し（Ｓ１０）、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出（Ｓ４０）しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断（Ｓ５０）し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信（ステップＳ６０）する。



【特許請求の範囲】

【請求項１】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知方法であって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知方法。

【請求項２】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知装置であって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを特徴とする不正利用通知装置。

【請求項３】　配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知プログラムであって、
流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、
流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、
流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、
不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを特徴とする不正利用通知プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、広範に流通するコンテンツの流通監視を行い、不正利用を検出して不正利用情報を通知する不正利用通知方法および不正利用通知装置に関する。

【０００２】

【従来の技術】従来の不正利用通知方法としては、電子透かし技術を用いてコンテンツを一意に識別できるコンテンツＩＤなどを予めコンテンツに埋め込でおいて流通させ、不正利用検出システムにより、正規配布先のＵＲＬと埋め込んだコンテンツＩＤとの対応関係をチェックして不正利用を監視するというネットポリス技術が知られている。

【０００３】このような不正利用検出システムにおいて用いられている検出技術としては、以下の技術が知られている。

【０００４】（１）透かし読み取り機能を有する探索ロボットにより、Ｗｅｂサイトのページに含まれているコンテンツをトップダウン的に探索する技術。

【０００５】（２）特定ネットワークに設けられた特定ノードのゲートウェーやサーバに透かし読み取りフィルタを組み込んでおき、このフィルタを通過するコンテンツを全てチェックする技術。

【０００６】（３）利用者のブラウザのダウンロードモジュールに透かし読み取りツールを予めプラグインしておき、ＷｅｂサーバからダウンロードしたコンテンツのコンテンツＩＤとアクセスサイトのＵＲＬをコンテンツＩＤ管理センタに通知してチェックする、ボトムアップ的な利用者協力型がある。

【０００７】例えば、エム研（http://www.mken.co.jp/）では、以下のようなサービスを行っている。

【０００８】このサービスでは、透かし検知ロボットにより、透かし入りコンテンツに関連しそうな単語をキーワードとしてサーチエンジンでピックアップしたＷｅｂサイトを中心に回るイエローリスト巡回方式と、著作権違反の可能性のあるコンテンツを持っているＷｅｂサイトを中心に回るグレーリスト巡回方式とに従って２４時間常時インターネットを監視しており、世界中のホームページを巡回して例えば、「acuaporta 」の電子透かしを埋め込んだコンテンツをデコードして監視し、不正にコピー、改竄されてネットワーク上に掲示されたコンテンツの発見に努めている。

【０００９】

【発明が解決しようとする課題】このように、従来の不正利用通知方法では、著作権保護技術によりカプセル化を行い、専用のソフトを利用して、鍵・利用条件・クライアント情報などの認証を行うことにより不正利用を防止していた。また、管理サーバに不正利用の疑いのあるコンテンツを転送し、コンテンツに予め埋め込んである

電子透かしなどを検出していた。

【００１０】しかしながら、従来の不正利用通知方法にあっては、管理サーバに不正利用の疑いのあるコンテンツを持ち込む必要があるので、インターネットの普及に伴って管理サーバの稼動負荷が増大するとともに、管理サーバの増設が必要になるといった問題があった。

【００１１】そこで、管理サーバの稼動負荷の増大や管理サーバの増設などを行なわずに、コンテンツを再生するクライアント側のメディアプレイヤに不正利用を検出して通知する方法が求められてきた。

【００１２】本発明は、上記に鑑みてなされたもので、その目的としては、クライアント側で自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる不正利用通知方法、不正利用通知装置および不正利用通知装置を提供することにある。

【００１３】

【課題を解決するための手段】請求項１記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知方法であって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【００１４】請求項２記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知装置であって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出手段と、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出手段と、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断手段と、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信手段とを有することを要旨とする。

【００１５】請求項３記載の発明は、上記課題を解決するため、配信されたコンテンツの流通過程での不正利用を検出して通知する不正利用通知プログラムであって、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出す読出ステップと、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出する算出ステップと、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断する判断ステップと、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信する送信ステップとを有することを要旨とする。

【００１６】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。

【００１７】図１は、本発明の一実施の形態に係る不正利用通知方法を適用可能なＤＲＭ処理フローの構成を示す図である。

【００１８】図１に示すように、本システムには、コンテンツを作成するためのエンコーダ装置１３、コンテンツを管理するためのＤＲＭ（Digital Rights Managemen t）装置１７、コンテンツを配信するためのメディアサーバ２１、コンテンツを再生するためのメディアプレイヤ２３が設けられている。

【００１９】エンコーダ装置１３は、一般に符号器と呼ばれ、カメラからのライブ画像、マルチメディアファイル、クライアント（パーソナルコンピュータ）の画面情報などのメディアファイルＡ１１を入力して一定の規則に従って符号化して指定形式の圧縮されたファイルに変換する機能を有しており、変換されたメディアファイルＢ１５が出力される。

【００２０】ＤＲＭ装置１７は、Ｗｅｂサーバからなり、Ｗｅｂサイトのメニューページや、情報の要求または支払いが行われる登録ページを提供して、登録ページ上から解凍のためのライセンスキーなどを与える機能を有している。特に、ＤＲＭ装置１７は、コンテンツを保護するためのライセンス管理や著作権管理機能によりコンテンツ管理を行っており、エンコーダ装置１３により変換されたメディアファイルＢ１５を入力して鍵番号とライセンスを取得するためのＵＲＬ情報を付加し、メディアファイルＢ１５に対して、エンコーダ装置１３による変換の逆変換を行うことが可能な鍵番号とライセンス取得ＵＲＬ情報を用いて暗号化して一体のデータになるようにカプセル化し、このカプセル化されたメディアファイルＣ１９をメディアサーバ２１に送信する。なお、カプセル化されたメディアファイル１９は、ライセンスとともに暗号化され「鍵」を用いなければ上述した逆変換が不可能なように保護されている。この「鍵」は、ＤＲＭ装置１７からメディアプレイヤ２３に別途配布される。

【００２１】また、カプセル化されたメディアファイル

１９を利用者にダウンロードさせるためにサーバ上のＷｅｂサイトに置いたり、ストリーミングのためにメディアサーバ２１上に置いたり、ＣＤ－ＲＯＭを媒体として配布したりする。

【００２２】メディアプレイヤ２３は、ＤＲＭ装置１７との通信機能をサポートしており、例えば、メディアサーバ２１からカプセル化されたメディアファイルＣ１９をダウンロードし、メディアファイルＣ１９から抽出した鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信し、ＤＲＭ装置１７からこの鍵番号とコンテンツＩＤに対応する鍵と利用条件およびクライアント情報などの証明書が返信され、カプセル化されたメディアファイルＣ１９がメディアファイル２５に逆変換され、ライセンスに含まれている利用条件に従ってメディアファイル２５がデコード機能により再生される。なお、ライセンスには、開始時刻、日付、期間、再生回数などのさまざまな権利行使するための利用条件を与えることができる。

【００２３】また、保護されたメディアファイルＣ１９を再生するためには、利用者はまずメディアファイルＣ１９をメディアファイルＢ１５に逆変換するためのライセンスキーを取得する必要がある。ライセンスキーの取得タイミングは、利用者が保護されたメディアコンテンツＣ１９を取得しようと試みたときや、メディアファイルを初めて再生したときに自動的に開始される。

【００２４】このときＤＲＭ装置１７は、Ｗｅｂサイトのメニューページから情報の要求または支払いが行われるＷｅｂサイト上の登録ページに利用者を誘導し、利用者は誘導された登録ページ上から解凍のためのライセンスキーを取得することとなる。

【００２５】また、メディアプレイヤ２３は、メディアファイルＣ１９を再生中に、このメディアプレイヤ２３が存在するクライアント（パーソナルコンピュータ）上のコンテンツＩＤに準拠したメディアファイルを順次参照して、後述する不正利用チェックフローによりのメディアファイルの不正利用があるかどうかを確認する。

【００２６】次に、図２は、コンテンツＩＤの詳細な構成に示す説明図である。

【００２７】詳しくは、図２に示すように、コンテンツＩＤには、コンテンツに関する属性情報を特定するためにコンテンツに一意的に付与される識別子として、左側から、コンテンツに一意に付与される番号（ユニークコード）を表すＩＤセンタ管理番号、コンテンツのクリエータや内容や種別や分類などに関する情報を表すコンテンツ属性、コンテンツの権利関係を表記する権利属性、権利の許諾・選任・確認に関する情報を表す権利運用属性、コンテンツの流通（＝売買）の履歴情報を表す流通属性、売買収益の分配に関する情報を表す分配属性、ＩＤ管理センタに任される自由領域を表す自由領域、ディジタル署名やコンテンツハッシュ値などを表すシステム領域などが設定されている。

【００２８】さらに、コンテンツＩＤの構成要素には、コンテンツを特定するための情報と流通に関する情報、電子透かしの方式などシステムに関する情報がある。これらの表現方法には、ユニークコード、流通記述子（ＤＣＤ：Distributed ContentDescription ）があり、必要に応じて使い分ける。なお、流通記述子（ＤＣＤ）は、コンテンツＩＤの中で権利者により予め規定された利用条件などの重要情報である。

【００２９】このうち、システム領域には、図３に示すように、コンテンツとコンテンツＩＤ（流通記述子：ＤＣＤ）をバンドルするためのディジタル署名とコンテンツハッシュ値が含まれており、これらを利用して不正チェックを行う。さらに、システム領域には、コンテンツデータと連結するためのコンテンツへのリンク、電子透かし情報、署名アルゴリズム情報、チェックディジットなどがある。

【００３０】ここで、ディジタル署名とコンテンツハッシュ値のデータ構造や数理的特徴を説明し、不正チェックをどのように行うかを説明する。

【００３１】図３に示すように、公開鍵暗号方式に基づいたデジタル署名においては、署名作成者がその通信内容となるコンテンツ（電子文書）を署名者固有の署名鍵（秘密鍵）により暗号化し、署名付きコンテンツ（電子文書）の受信者がその署名鍵に対応する署名作成者の検証鍵（公開鍵）によりそのデジタル署名が本当に送信者の署名であるのかどうかを検証することができるという仕組みになっている。

【００３２】従って、デジタル署名は、通信内容を暗号化したものを署名とするという技術的な特性から、署名そのものと通信内容である電子文書自体との結合性が強く、もし通信内容が通信途上で改竄されれば、後述する署名の検証過程によって、改竄されたという事実も検証することができるという利点がある。

【００３３】具体的な実現方法の１つであるクリアディジタル署名（分離署名）は、図３に示すように、コンテンツデータとディジタル署名が分離されており、コンテンツデータはそのまま読め、一方、ディジタル署名が記述されているシステム領域には、コンテンツ本文のコンテンツハッシュ値（秘密の計算式で計算した値）を含んでいる。

【００３４】このため、ディジタル署名が改竄された場合には、ディジタル署名の署名対象となるコンテンツハッシュ値も同時に改竄されることになる。その結果、実際のコンテンツハッシュ値を計算して、計算されたコンテンツハッシュ値とコンテンツＩＤ中のコンテンツハッシュ値が異なり、ディジタル署名の改竄を検出することができる。

【００３５】ここで、図３に示すコンテンツハッシュ値は、予め決められたハッシュ関数により得られた値であ

り、ハッシュ関数には、不可逆な一方向関数を含むため、コンテンツハッシュ値からコンテンツデータを再現することはできず、また同じコンテンツハッシュ値を持つ異なるコンテンツデータを作成することは極めて困難である。なお、ハッシュ関数としては、例えば、ＭＤ５、ＳＨＡ１などが広く知られている。

【００３６】また、具体的な検出過程では、このハッシュ関数は、与えられたコンテンツデータから固定長の疑似乱数を生成する演算手法であり、通信などの流通過程を通じてコンテンツデータを提供する際に、流通前のコンテンツデータからハッシュ関数を用いて求めておいたコンテンツハッシュ値をコンテンツＩＤのシステム領域から抽出しておき、流通後のコンテンツデータからハッシュ関数を用いて求めたコンテンツハッシュ値と比較すれば、コンテンツデータが通信などの流通途中で改竄されているかどうかを調べることができる。

【００３７】次に、図４は、コンテンツの作成時におけるコンテンツＩＤの埋め込みフローである。

【００３８】図４に示すように、メディアファイルＡ１１として、音声ファイルに関してＷＡＶ．ＷＭＡ．ＭＰ３などの識別子があり、映像ファイルに関してＷＭＶ．ＡＳＦ．ＡＶＬ．ＭＰＥＧ１などの識別子があり、その他のファイルの識別子としてＢＭＰがある。メディアファイルＡ１１は、二階層電子透かしをオプションとして扱うことができる。

【００３９】エンコーダ装置１３で変換されたメディアファイルＢ１５として、ＷＭＡ，ＷＭＶ，ＡＳＦなどの識別子があり、これらのカプセル化されたメディアファイルＢ１５のヘッダ情報へ上述したＤＣＤを埋め込む。

【００４０】ＤＲＭ装置１７でカプセル化されたメディアファイルＣ１９は、上述したＤＣＤをバインドする。

【００４１】なお、メディアファイルＡ１１は、ＩＤセンタ管理番号からなるユニークコードを用いた二階層電子透かしをオプションとして扱うことができる。

【００４２】ここで、二種類の異なる電子透かしを順次埋め込む二階層電子透かしについて説明する。

【００４３】電子透かしには、多数の方式があり、すべての電子透かしを順次試みるとなると、検出時間が膨大になってしまう恐れがあるため、メタ電子透かしを用いて実電子透かしの種別情報を埋め込むようにする。この実電子透かしは、ＩＤセンタの管理番号を埋め込むものであり、メタ電子透かしは、実透かしの種別情報を埋め込むものである。

【００４４】検出手順は、メタ電子透かしの検出により実電子透かしの種別を特定し、さらに、特定した実透かしを検出するようにするので、二種類の異なる電子透かしにより埋め込まれたユニークコードの検出過程を複雑化でき、不正利用者による容易な解読をできないようにすることができる。

【００４５】なお、ユニークコードは、ＩＤセンタ管理番号を示しており、その構成は以下の通りである。

【００４６】（１）地域コード（4bit）
世界を１６地域に分割してセンタの番号付与が可能である。

【００４７】（２）センタ番号（8bit）
Registoration Authority が発行し、ＩＤセンタを識別する固定長の番号である。

【００４８】（３）センタ内番号（任意）
ＩＤセンタが管理するコンテンツを識別する番号であり、ＩＤセンタが任意に割付ける。

【００４９】（４）バージョン番号（4bit）
コンテンツＩＤのバージョンを２進数によるバイナリ表現を用いて規定した番号である。

【００５０】次に、図５は、メディアプレイヤ２３の機能構成を示す図である。

【００５１】メディアプレイヤ２３は、メディアファイル２５の再生中に、メディアプレイヤ２３が存在するクライアント上のコンテンツＩＤに準拠したファイルを順次チェックし、不正利用のメディアファイルを確認する。

【００５２】図５に、メディアプレイヤ２３の機能構成の一例を示す。メディアプレイヤ２３は、認証部４１、流通情報蓄積部４３、不正利用チェック部４５、メディア再生部４７から構成されている。

【００５３】また、メディアプレイヤ２３により再生されるメディアファイルは、先頭からヘッダ情報、システム化領域、ディジタル署名、コンテンツハッシュ値、コンテンツ領域を有している。

【００５４】認証部４１は、入力されたメディアファイルから鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信し、ＤＲＭ装置１７から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。

【００５５】流通情報蓄積部４３は、過去に再生したメディアファイルのコンテンツＩＤから収集した流通属性を流通情報として蓄積する。

【００５６】不正利用チェック部４５は、クライアント上のメディアファイルをサーチし不正利用を検出するモジュールであり、その詳細な動作を図６に示す不正利用チェックフローにより処理される。

【００５７】メディア再生部４７は、ＤＲＭ装置１７から受信した利用条件に従ってメディアファイル２５をデコード機能により再生する。このデコード機能は、エンコーダ装置１３による符号化とは逆に、符号化されたメディアファイル２５をメディアファイルＡ１１に復号する機能である。

【００５８】ここで、図５に示すメディアプレイヤ２３での基本的な動作を説明する。

【００５９】なお、パーソナルコンピュータからなるクライアントには、制御部にＯＳプログラムや制御データやアプリケーションプログラムを一時的に記憶するＲＡ

Ｍと、制御プログラムやアプリケーションプログラムに従ってシステムを制御するＣＰＵとが設けられている。また、ハードディスクＨＤに記録されているアプリケーションプログラムは、例えばパーソナルコンピュータに設けられたＣＤ－ＲＯＭドライブなどを用いてＣＤ－ＲＯＭなどの記録媒体からインストールされたプログラムであり、本発明の不正利用通知プログラムを記録した記録媒体などである。

【００６０】クライアント上でメディアプレイヤ２３の画面からメディアサーバ２１のＵＲＬを指定してホームページを開き、メディアファイルを受信する。そして、認証部４１では、入力されたメディアファイルから鍵番号とコンテンツＩＤを抽出してＤＲＭ装置１７に送信する。そして、認証部４１が、ＤＲＭ装置１７から鍵・利用条件・クライアント情報などの証明書を受信して認証を行う。そして、メディア再生部４７では、メディアファイル２５をＤＲＭ装置１７から受信した開始時刻、日付、期間、再生回数などの利用条件に従ってメディアファイルＡ１１に復号して再生する。

【００６１】このメディア再生部４７でメディアファイルの再生を行っている際に、並行して不正利用チェック部４５は、バックグラウンドでクライアント上にある他のメディアファイルを対象にした不正利用チェックを行う。

【００６２】図６において、不正利用チェックを開始すると、ステップＳ１０では、メディアファイル２５のコンテンツＩＤからヘッダ情報を読み込み、特に、流通後のメディアファイルに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値とディジタル署名を読み出す。

【００６３】そして、ステップＳ２０では、ディジタル署名の改竄チェック処理を行う。

【００６４】すなわち、流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を計算して、計算された流通後のコンテンツハッシュ値とコンテンツＩＤ中に記述されている流通前のコンテンツハッシュ値が異なった場合には、ディジタル署名の改竄があったこととなる。

【００６５】そして、ステップＳ３０では、改竄があるかどうかを判断する。改竄がない場合には、ステップＳ４０に進み、流通後のコンテンツに対して流通前に記述されたコンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いて流通後のコンテンツハッシュ値を算出する。

【００６６】そして、ステップＳ５０では、算出した流通後のコンテンツハッシュ値がメディアファイル２５のコンテンツＩＤから読み出した流通前のコンテンツハッシュ値と不一致かどうか判断する。

【００６７】ここで、算出した流通後のコンテンツハッシュ値がメディアファイル２５の流通前のコンテンツハッシュ値と一致した場合には、正常な利用であることを示しているので、そのまま処理を終了する。

【００６８】一方、ステップＳ３０で改竄があると判断した場合、または、ステップＳ５０で流通前後のコンテンツハッシュ値同士が不一致の場合、ステップＳ６０に進み、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信し、処理を終了する。

【００６９】このように、不正利用チェック部４５において、メディアファイル２５のディジタル署名とコンテンツハッシュ値の確認を行うので、当該メディアファイル２５が不正利用かどうかを検出することができ、当該メディアファイル２５が不正利用の場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することができる。

【００７０】また、コンテンツＩＤに示されるセンタアドレス（センタサーバのＵＲＬ）に、不正利用があったことを示す不正利用情報を通知することができる。なお、この不正利用情報には、コンテンツＩＤと存在場所（端末のＩＰアドレス）、不正利用チェック結果を含むこととする。

【００７１】この結果、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができ、特に、メディアプレイヤに適用することができる。また、クライアント側の不正監視手段として適用することができる。

【００７２】また、メディアプレイヤのバージョンアップに合せて、新しいディジタル署名方式や新規チェック項目を追加した場合でも、不正利用検出フローを容易に改定することができる。

【００７３】本実施の形態における効果は、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【００７４】

【発明の効果】請求項１乃至３記載の本発明によれば、流通後のコンテンツに添付されているコンテンツＩＤから流通前に記述されたコンテンツハッシュ値を読み出し、流通後のコンテンツに対して流通前に記述された前記コンテンツハッシュ値の算出に用いたハッシュ関数と

同一のハッシュ関数を用いてコンテンツハッシュ値を算出しておき、流通前後のコンテンツハッシュ値に対して両者が一致するかどうかにより不正利用があるかどうかを判断し、不正利用があった場合には、コンテンツＩＤに含まれる管理サーバのアドレスに不正利用があったことを示す不正利用情報を送信することで、自由にダウンロードされたコンテンツに対して、利用者に意識させることなく不正利用の監視を行うことができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る不正利用通知方法を適用可能なＤＲＭ処理フローの構成を示す図である。

【図２】コンテンツＩＤの詳細な構成に示す説明図である。

【図３】ＤＣＤの詳細な構成に示す説明図である。

【図４】コンテンツ作成時のコンテンツＩＤの埋め込みフローである。

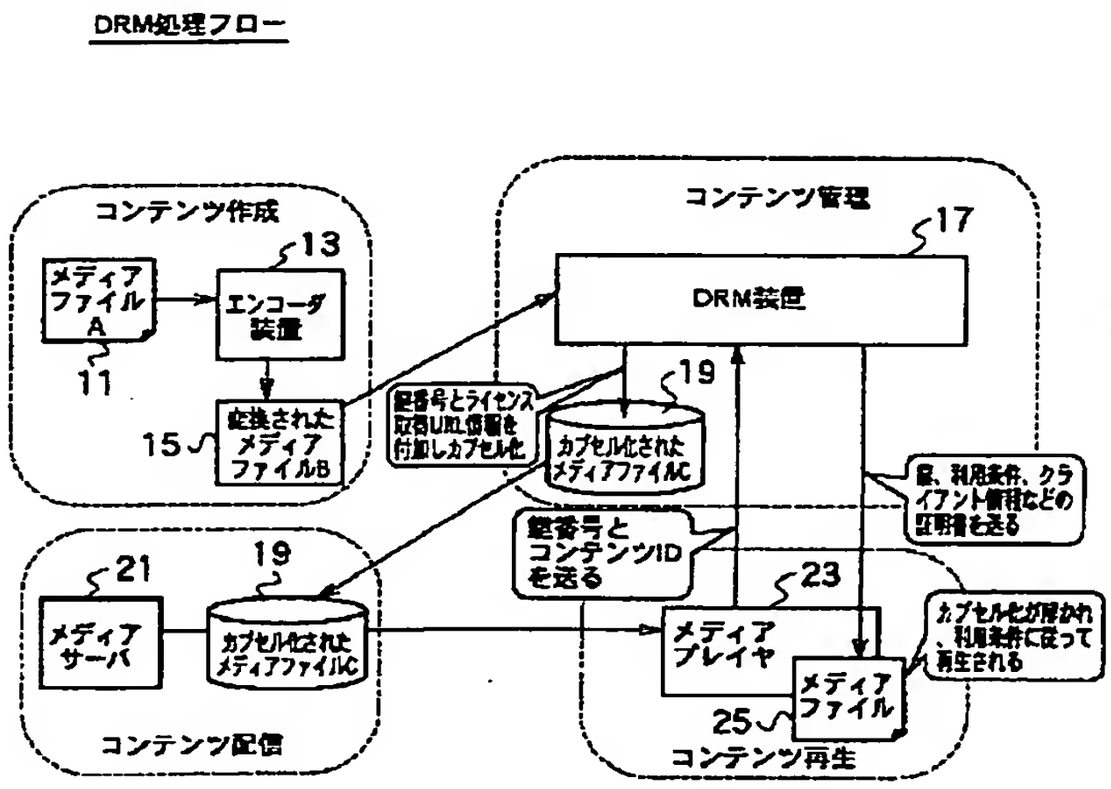
【図５】メディアプレイヤ２３の機能構成を示す図である。

【図６】不正利用チェック部４５の詳細な動作を説明するためのフローである。

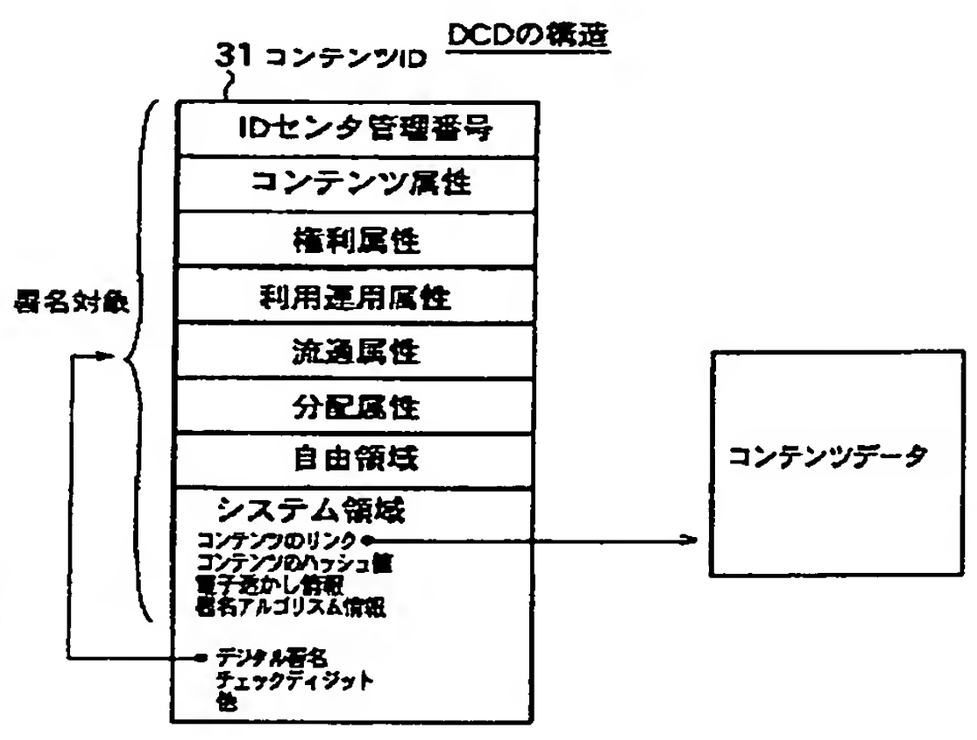
【符号の説明】

１３　エンコーダ装置
１７　ＤＲＭ装置１７
２１　メディアサーバ
２３　メディアプレイヤ
２５　メディアファイル
３１　コンテンツＩＤ
４１　認証部
４３　流通情報蓄積部
４５　不正利用チェック部
４７　メディア再生部

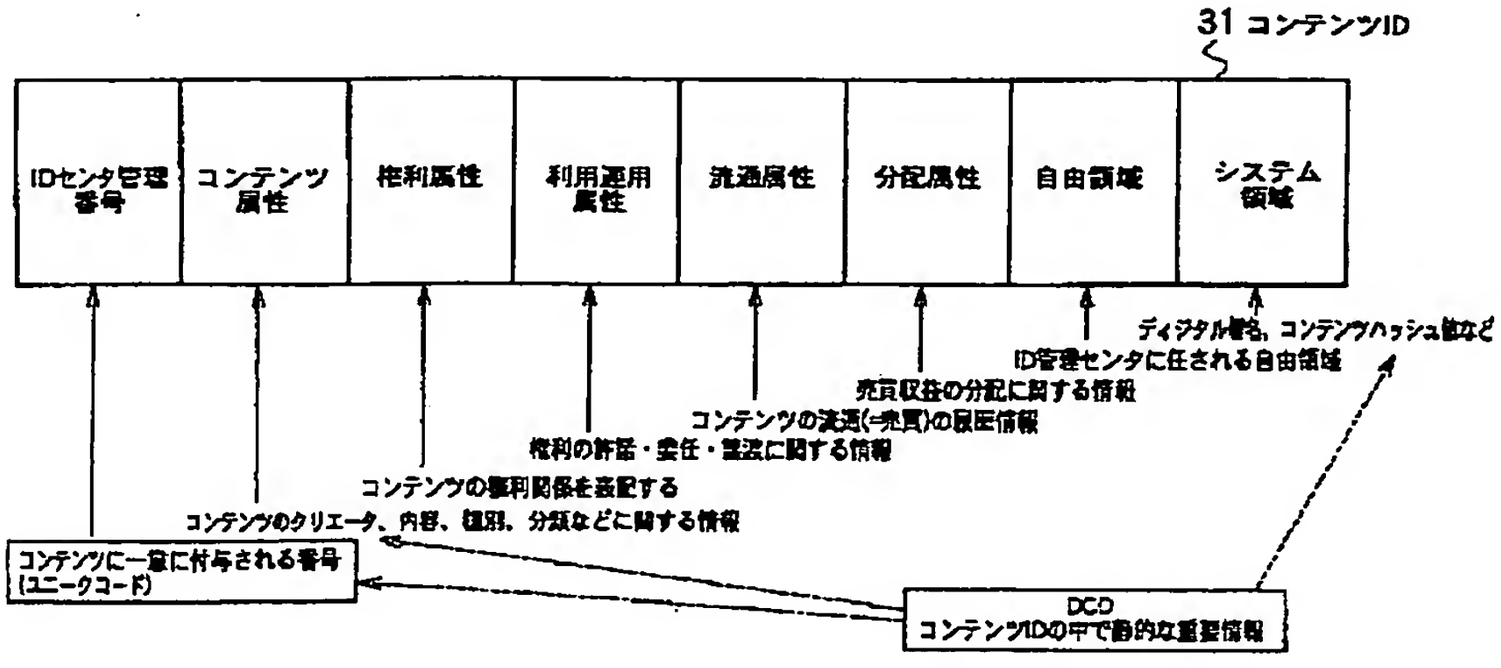
【図１】



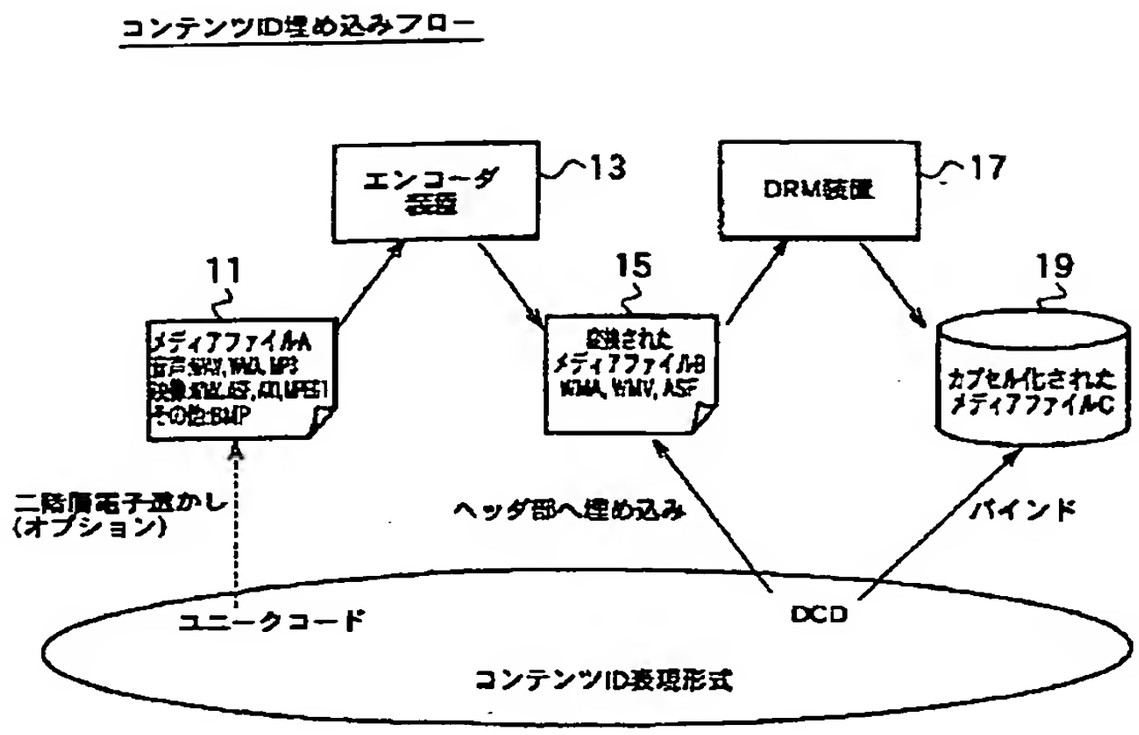
【図３】



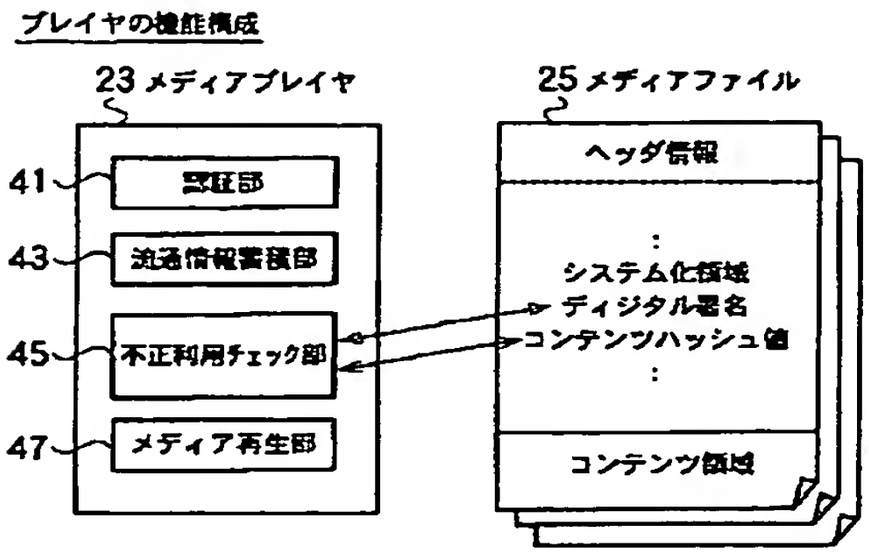
【図２】



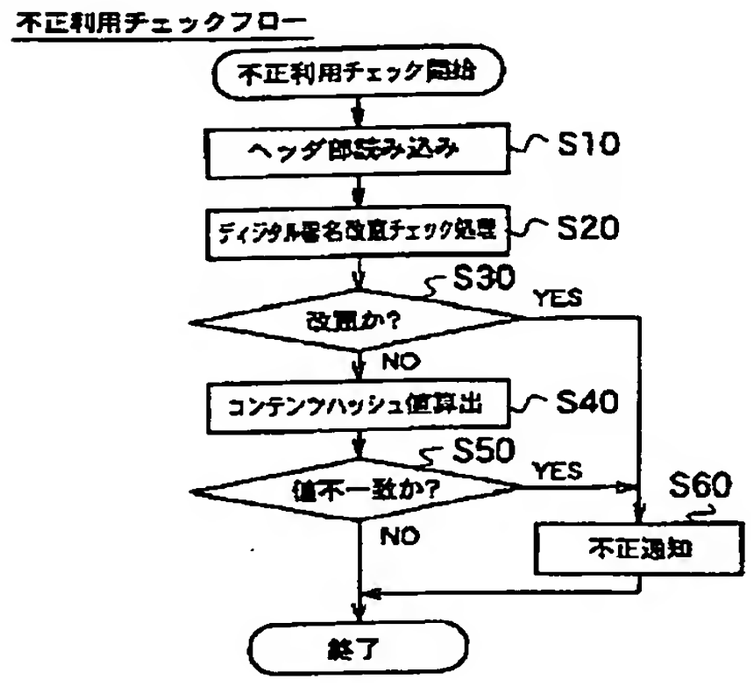
【図４】



【図５】



【図６】



フロントページの続き

(72)発明者　佐野　睦夫
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5B085 AE00
5J104 AA08 AA13 LA02 LA05 NA12 PA14